EURASIP Journal on Image and Video Processing

RESEARCH Open Access

Research on digital image encryption algorithm based on double logistic chaotic map

Hailan Pan[1,2,3*], Yongmei Lei[1] and Chen Jian[2,3]

Abstract

With the development of information technology, image information has become the main content of network information transmission. With the development of image encryption technology, it is also about the development of image information theft technology. In order to cope with the evolving information theft technology, we must seek a better image encryption algorithm. Among many algorithms, due to the superiority of chaos technology, when the image is encrypted with chaos technology, the ciphertext presents a randomness, which makes the possibility of deciphering greatly reduced. Therefore, the research of digital image encryption algorithm based on chaos technology has become an important means of modern digital image encryption. In this paper, the digital image encryption technology is studied with the dual logistic chaotic map as a tool. The simulation experiments are carried out by using the classical Lena image and the life picture, and the results are analyzed from the histogram, pixel correlation, information entropy, key space size, key sensitivity, and so on. The results show that the method used in this paper has a better security effect.

Keywords: Chaos technology, Logistic mapping, Digital image, Encryption

1 Introduction

In recent years, along with the rapid promotion and popularization of network technology and digital communication technology in the world, digital images, and digital video-based digital images have become an important medium for information storage and transmission in the computer network in the civil and military fields. However, network security issues have long been an important factor that plagued and restricted the development of network technology. Especially in the context of the information resources of the public and government departments, how to realize the data security protection in the computer network is the important content and direction of the research in the field of network security and information security. Among them, digital image and digital video have become the important content of data transmission in the network by virtue of its intuitiveness and convenience. Therefore, the security protection of digital images has received great attention from all parties. Especially in the background of the increasingly severe network security situation in recent years, information transmission and sharing based on digital images often face the problems of data theft, tampering, deletion, and attack, which have caused great losses to the owners or publishers of digital images.

In the security system of digital information, encryption technology is a very common technique and method. Encryption technology can be encrypted by encrypting the original data. If the security and reliability of the encryption method is high enough, then the security of digital information can be protected [1–4]. Therefore, the research on digital image encryption technology and method is an important direction for digital image security protection. However, encryption technology or encryption system is mainly based on the requirements of text encryption. At present, the more common encryption system cannot achieve better results in the compatibility and encryption quality of digital image encryption.

* Correspondence: panhailan@sspu.edu.cn
[1]School of Computer Engineering and Science, Shanghai University, No. 99, Shangda Rd, Baoshan District, Shanghai, China
[2]Research Center of Resource Recycling Science and Engineering, Shanghai Polytechnic University, No. 2360, Jinhai Rd, Pudong New District, Shanghai, China
Full list of author information is available at the end of the article

Although digital images can be processed as a two-dimensional data set, cryptographic systems that directly use text-encryption techniques often face problems of inefficiency in encryption and decryption, low practicability, and low security [5–8]. Researching a cryptographic system or encryption method suitable for digital image encryption is the only way to protect the security of digital images in the network environment. In the field of secure encryption of digital images, two kinds of technical means are generally used:

1) Digital watermarking technology, namely Digital Watermarking Technology. The technology adopts the signature processing of digital images and adds custom watermark information to the original digital images to protect the copyright of digital images. It is one of the important technical means for image security protection in the Internet. However, the disadvantage of digital watermarking technology is that the visibility of digital images cannot be avoided. Usually, only the copyright of the image is not infringed, and when the content of the digital image needs to be protected, there is nothing that can be done.
2) The digital image protection method is image encryption technology [9–13], and its basic principle is to encrypt the digital information contained in the digital image, and get the completely different encrypted images of the appearance and the original digital image, so that the content of the digital image cannot be viewed directly. When the digital image is needed for viewing or using, the corresponding decryption algorithm is used to calculate and decrypt the encrypted image to restore the original content of the digital image, which is an important means for digital image content protection in a distributed environment with high security requirements.

With the increasing demand for image encryption, many domestic and foreign scholars have proposed many different encryption techniques and methods in the field of digital image encryption. Typical algorithms or techniques in common use mainly include digital image encryption based on pixel transformation, digital image encryption based on random sequence, digital image encryption based on image compression coding, and digital image encryption based on image key. The chaos technology is difficult to crack and randomness, which makes the digital image encryption technology based on chaos technology become a more reliable digital image encryption technology. Many researchers have introduced chaos concept to improve the precision and security of chaos technology. In the 1980s [14], British mathematician Matthews first proposed an encryption method based on logistic chaotic system. In Matthews' encryption method, the encryption technology type is stream encryption technology, which specifically combines chaotic power and cryptography. Although the encryption technology and method cannot meet the commercial requirements in terms of encryption precision, encryption security capability, and actual encryption efficiency, it plays a vital role in the development and application of chaotic encryption technology. Then, Toshiki Habutsu [15], a Japanese scholar, published the iterative encryption method of chaotic cipher in European cryptography conference, which is a major breakthrough for chaotic encryption technology. Subsequently, the cryptography community's research on chaotic encryption technology developed rapidly. American scholar Fridrich [16] proposed a chaotic encryption technology and method based on two-dimensional Baker mapping and applied it to the encryption and protection of digital images. It is the first application and practice of chaotic encryption in the field of digital image encryption [17–21]. In order to improve the security and reliability of chaotic encryption technology, some scholars have extended the two-dimensional chaotic encryption method to realize chaotic encryption methods in three-dimensional space and multidimensional space [22–27]. However, in the three-dimensional chaotic encryption process, the scrambling operation and the obfuscation operation processing steps are still processed in an isolated manner, and fixed control parameters are adopted in the processing, so that the chaotic encryption algorithm and method still appear to be broken.

From the overall situation, the research results in the field of digital image chaos encryption are relatively rich, and it has also greatly promoted the rapid development and application of digital image encryption technology. However, the current image chaotic encryption technology still fails to break through the category of two-dimensional integer-order chaotic systems, and there is still room for improvement in dynamic characteristics and pseudorandomness. The chaos encryption technology based on high dimension space proposed by some scholars has the problems of poor uniformity of pixels in the process of encryption, the difficulty of confusion processing, and the low efficiency of encryption and decryption process.

This paper proposes a digital image encryption method based on double logistic chaotic map. In the double chaotic digital image encryption, second-level logistic chaotic map is mainly used to create and generate pseudorandom sequence numbers, and the number of random sequences of image confusion and scrambling is obtained through two creation processes. In the process of encryption and decryption, the key used in the double chaotic digital image encryption method is the calculation parameter of the first-level logistic chaotic map and the initial value of

the second-level logistic chaotic map. The encryption process is performed in the order of confusion and scrambling, and the decryption process is processed in the reverse order. The simulation results of the picture show that the histogram, pixel correlation, information entropy, key space size, and key sensitivity all reach a high level, and the image decryption processing can be completed basically correctly.

2 Proposed method

2.1 Chaos technology

Chaos theory is a non-deterministic theoretical system based on nonlinear systems and randomness. The definition of chaotic system is as follows:

1) The period of $f(x)$ does not have an upper bound;

2) Let S be an uncountable subset of I, then the following conditions are true:

$$\forall x, y \in S, x \neq y, \lim_{n->\infty} \sup \mid f^n(x) \mid -f^n(y) \mid > 0$$

$$\forall x, y \in S, \lim_{n->\infty} \inf \mid f^n(x) - f^n(y) \mid = 0$$

$$\forall x \in S, \lim \sup_{n>\infty-} \mid f^n(x) - f^n(y) \mid > 0$$

(y is any periodic point of f(x))

The $f(x)$ that satisfies the above relationship is called the chaotic system on S, in which the set of limit points has both scattered and concentrated characteristics. At the same time, for any periodic point of the mapping function $f(x)$, there is no correlation in all subsets. The essence of the chaotic system belongs to a nonlinear system, but compared with the usual nonlinear system, the chaotic system has some unique characteristics, which mainly include the boundedness, ergodicity, internal randomness, initial value sensitivity, and fractal dimension.

In chaotic systems, logistic mapping is an important chaotic system. Logistic mapping, also known as insect population mapping, is a nonlinear iterative equation. It is an example of the most commonly used chaotic system in chaos research. Its definition is as follows:

$$x_{k+1} = \mu x_k (1 - x_k), x_k \in (0, 1) \quad (1)$$

Logistic mapping can express the quantitative breeding model of insects, that is, the number of offspring of insects in the breeding process far exceeds the number of parents. So if the offspring insects are born, the number of parental insects can be almost ignored, and the logistic map appears different according to the parameters. When the logistic is mapped when the parameter μ satisfies the condition $\mu \in (3, 4]$, the chaotic sequence will be generated. The characteristic of the sequence is very similar to that of white noise. It is commonly used in the chaotic encryption of digital images before H.

It can be found from the definition and characteristics of the chaotic system that the chaotic system is very sensitive to the initial value. In a cryptographic system, if the subtle changes in the key can lead to obvious changes in the encryption results, the encryption algorithm or the cryptographic system has a better encryption effect, that is, the high sensitivity to the existence of the key. Therefore, with the sensitivity of the chaotic system to the initial value, an encryption system based on chaotic systems can be constructed. At present, the encryption technology based on chaos is mainly divided into two types. The first type is a secure communication encryption system based on chaotic synchronization technology. The second type is a digital encryption system based on the chaotic system to create a stream encryption key or the homogeneous group key. Due to the orbital hybrid type and initial value sensitivity characteristics of chaotic systems, the hybrid characteristics of the chaotic system can be applied to the confusing processing in the encryption process, and the chaotic characteristics of the chaotic system corresponded to the pseudorandomness and key-sensitive demand required by the encryption system. At present, most chaotic mapping applications in encryption technology use the mapping reference algorithm which is more commonly used in traditional cryptography.

The digital image chaotic encryption technology is to use chaotic mapping to encrypt and protect the digital image and to design the corresponding decryption method. At present, the digital image encryption technology or method based on the chaotic system mainly uses the chaotic mapping to create the pseudorandom sequence, different from the traditional method of using computer software to create pseudorandom number. As long as the same initial value is set in the data encryption technique based on a chaotic system, the sequence of pseudorandom number is exactly the same and the randomness of the sequence is better. In the digital image chaotic encryption system, the encryption can be realized by using the pseudorandom number sequence generated by the image pixel set and chaos, and the decryption process can perform the inverse operation.

2.2 Double chaotic digital image encryption method

According to the modern cryptosystem, the encryption and decryption process is realized by the transformation operation of the encryption key and the decryption key. The target of the encryption is the plaintext space, and the target of the decryption is the ciphertext space. For the cryptographic framework of the digital image, the plaintext space P corresponds to the set of pixels of the original digital image that needs to be encrypted, and the ciphertext space C corresponds to the set of image pixels after the encryption. The ciphertext space C obtained by the plaintext space P after encryption can be transmitted

in an insecure channel. The key K is a key for performing an encryption transform operation and a decryption transform operation. The same key may be used for different encryption keys and decryption keys according to the selected encryption method, or different keys may be used. In the key space {K}, the control implementation of the encryption algorithm is realized, which is a space composed of the basic information grasped by both the plaintext space and the ciphertext space. The main flow based on the double chaotic image encryption method is shown in Fig. 1.

The two chaotic sequence generators included in the encryption and decryption process of Fig. 1 are the key modules of the encryption system. It is responsible for the realization of the image encryption algorithm of the system. It is implemented by two chaotic maps, so it is called the double chaotic digital image encryption system, and the other modules mainly include the encryption and decryption module and the transmission module.

2.2.1 Random sequence generation

Since the random number generation method in the computer cannot achieve complete randomness, the sequence obtained by chaotic mapping is a pseudorandom sequence. In the random sequence generator module of the digital image chaotic encryption system in this paper, the choice of chaotic map is an important issue. In this paper, the logistic mapping method is adopted as the pseudorandom sequence generator. The distribution function of the logistic pseudorandom sequence is shown in the following formula:

$$\rho(x) = \begin{cases} \left(\pi\sqrt{1-x^2}\right)^{-1} & x \in (0,1) \\ 0 & x \notin (0,1) \end{cases} \tag{2}$$

In the specific random sequence generation module, this paper sets up two logistic maps (L1 and L2) for the iterative creation of pseudorandom sequences, in which L1 is used for the creation of a pseudorandom sequence of the first level and L2 is used for the creation of a pseudorandom sequence of the second level. The corresponding random number sequence is automatically generated according to the initial value setting and is used for stream encryption processing of the digital image.

2.2.2 Encryption and decryption module

The image encryption process of the double chaotic digital image encryption system in this paper includes two processes of confusion processing and scrambling processing. The confusion processing is to XOR the pixel matrix of the image with the number of pseudorandom sequence X and the scrambling processing is also processed by the pseudorandom sequence data obtained by

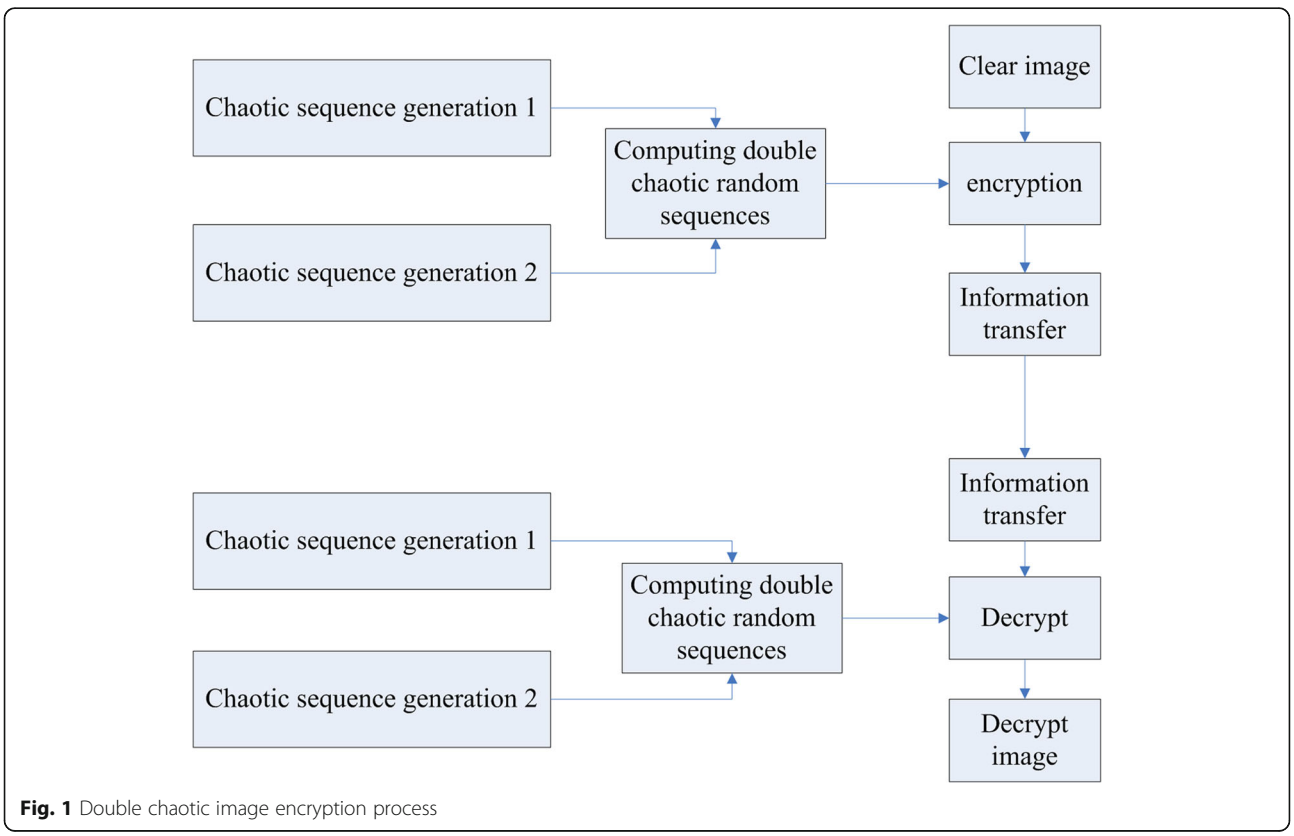

Fig. 1 Double chaotic image encryption process

the logistic chaotic map. The confusion processing method is as follows:

1) Submit the initial values a and b for the pseudorandom sequence number calculation model, and set the calculation parameter $\mu_1 = 3$ of L1 to calculate the pseudorandom sequence number X.
2) Calculate all the elements of the pseudorandom sequence number in $(x_i \times 256) \bmod 256$, and then convert the calculated result into binary, thereby obtaining a binary $M \times N$ long sequence number.
3) Get the pixel gray or color component sequence of the digital image to be encrypted and get the gray or color component sequence vector G of the digital image.
4) For the first element g_i in G, XOR is performed according to $X^{'} \oplus g_i$. For subsequent elements in G, it is calculated according to the following formula:

$$I^{'}(k) = X^{'(k)} \oplus \left\{ \left[X^{'(k)} + g_k \right] \bmod N \right\} \oplus I^{'}(k+1) \quad (3)$$

where k represents the k pixel in the image.

5) Reverse the pixel sequence obtained in the fourth step, and adjust the original $M \times N$ elements to the first position, and adjust the original $M \times (N-1)$ elements to the second position. Then, according to formula 3, the second obfuscation process is performed.

The image scrambling method is as follows:

1) Using the pseudorandom sequence number X of the confusion process as the final set X of pseudorandom sequence numbers.

2) The I is homogenized and an empty vector Y of $M \times N$ size is set, and the X corresponding element is extended to the integer domain space of $(0, M \times N)$ according to the homogenization of the X element, and the result is written to the vector Y.

3) Using the vector Y obtained in the previous step and the encrypted image I' after the confusion process, the pixel is scrambled for I'. That is, the gray value of the ith pixel and the gray value of the y_ith pixel in I' are exchanged.

4) The result of scrambling is again subjected to a round of positive order confusion and reverse order confusion according to the fourth and fifth steps in the confusion process, thereby obtaining the final encrypted image I''.

According to the above confusion and scrambling process, the double chaotic digital image encryption system adopts the method of first confusing and then scrambling to encrypt the image. The process of image decryption is performed by first scrambling and then confusing, and the operation is the inverse operation of the above process. In the case of confusing inverse processing, the following methods are used.

$$g_k = \left\{ X^{'}(k) \oplus I^{'}(k) \oplus I^{'}(k-1) - X^{'}(k) \right\} \bmod N \quad (4)$$

2.3 Security analysis of digital image encryption

The evaluation of the encryption algorithm is mainly to evaluate the security of the encryption algorithm. The security evaluation of this paper is mainly analyzed from the randomness of the sequence and the effect of mapping scrambling.

The number of random sequences has a very important impact on the security of digital image encryption. The pseudorandom signal generated by the chaotic system has the characteristics of high initial sensitivity, randomness, and unpredictability. It is very suitable for application in the encryption system. Therefore, the encryption system based on chaotic system is very widely used in practical applications. At present, in practical applications, chaotic sequences are created and generated by using chaotic systems, and then the chaotic sequences and encrypted data are coded or fused, and the encrypted ciphertext sequence is obtained. The chaotic encryption system belongs to the symmetric encryption system. In the process of data decryption, the same chaotic system and initial value are needed to create the pseudorandom sequence number, and then the ciphertext sequence is calculated correspondingly to obtain the plaintext sequence. It is very efficient and fast to encrypt data by using pseudorandom sequence number of chaotic map. However, with the development and advancement of information security technology, the problem of the key sequence security of the encryption system based on a single chaotic map has been gradually convex. Because the chaotic encryption sequence is generated by chaotic mapping, since there are only 10 types of chaotic systems, the attacker can analyze the chaotic system used in the encryption process based on the item space construction method. Unless the entire encryption process is absolutely safe, the attacker can crack the parameter values and initial values of the chaotic sequence based on certain plaintext and ciphertext pairs, thus breaking the encryption algorithm.

The double chaotic image encryption algorithm proposed in this paper adopts a track jump method similar to Rowlands in the production process of random sequence numbers. It is a two-layer iterative method constructed by a double chaotic system. There is an initial value correlation between the first-order chaotic map and the second-order chaotic map, and the two random sequence numbers are recalculated in the calculation process. The obtained random number sequence not only contains

sequence fragments generated by different initial values, but also increases the period length of random sequence number through periodic fusion, which can effectively alleviate the problem of insufficient randomness caused by limited computer precision. In addition, a prominent feature of the chaotic encryption algorithm is the initial value sensitivity. Even if the same encryption method is used, as long as the initial values are different, the number of random sequences obtained will be completely different.

The main process of chaotic image encryption algorithm includes two processes of confusion and scrambling based on the number of pseudorandom sequences. Whether it is the confusion of pixel color processing or the scrambling process of pixel position conversion, the processing effect is highly correlated with the randomness of the number of pseudorandom sequences. Therefore, the pseudorandom number generator of this paper is analyzed by simulating the scrambling operation. The random analysis of the scrambling location in this paper is mainly through the construction of the scrambling matrix which satisfies the sequence number of uniform distribution after the random sequence number is optimized, and the $M \times N$ matrix is obtained, and then the randomness of the scrambling matrix is examined by the correlation between the eight neighborhood elements of the elements of the scrambled matrix.

3 Experimental results and discussions

The original digital image selected in the experimental simulation includes a total of 10 sample images. At the same time, because the encryption effect of the algorithm is independent of the image size, the pixel width and height of all the test samples are 490 and the number of pseudorandom sequences is 65,536 for the efficiency of the algorithm. In this experiment, a round of scrambling

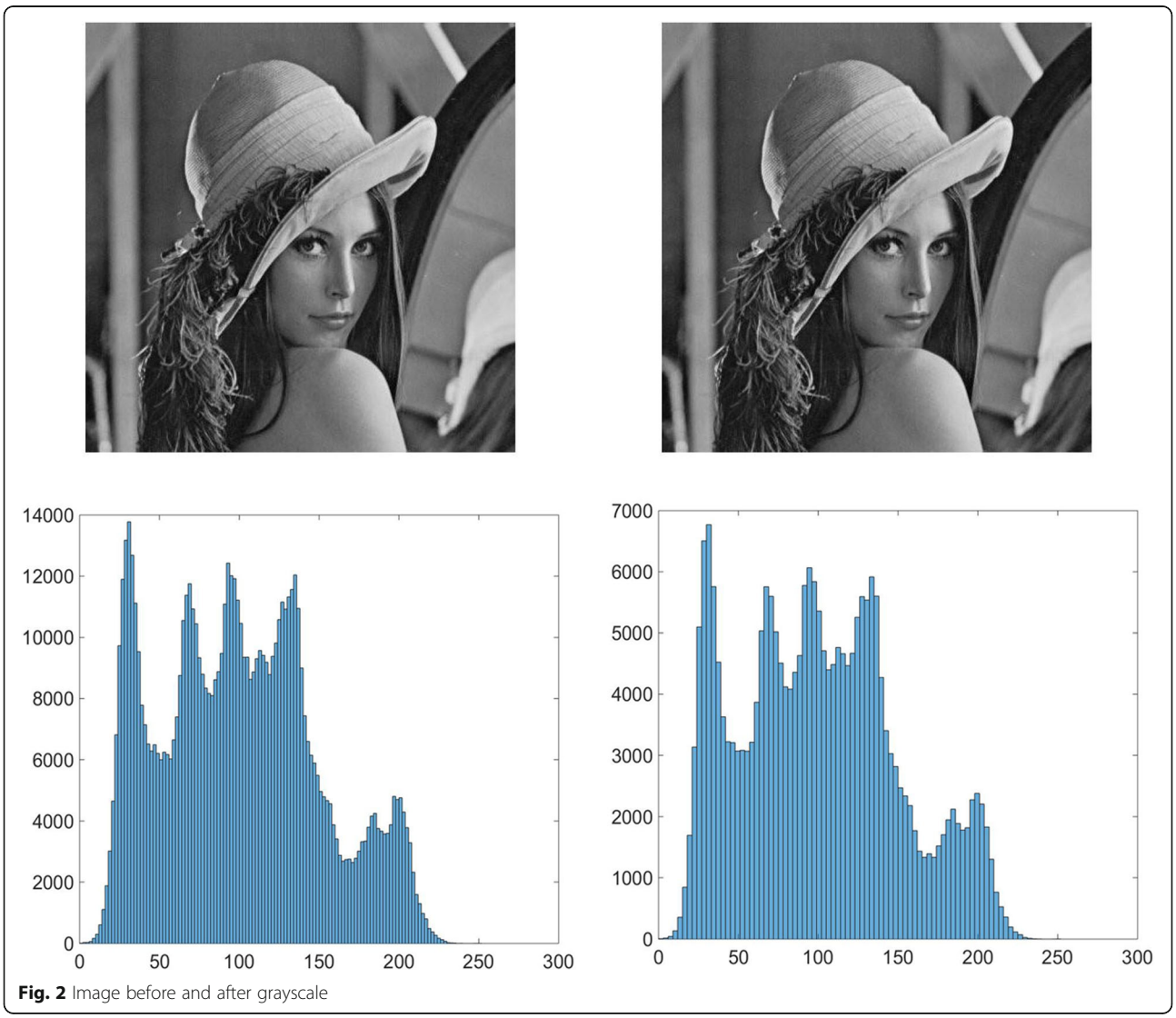

Fig. 2 Image before and after grayscale

was performed and the diffusion process was operated twice. The original image is a three-dimensional array. As shown in Fig. 2, the top left of Fig. 2 is the Lena original image. For the image of 490 × 490 in this paper, it is digitally stored as a matrix of 490 × 490 × 3. In order to achieve digital encryption better, it must be grayscaled. The image after graying as shown on the upper right side of the figure is a 490 × 490 array. From the image, there is no difference between the original image and the grayscale image, but from the histogram, there is a certain difference between the two. The lower left of Fig. 2 is the histogram of the original image, and the lower right of Fig. 2 is the histogram of the grayscale. It can be seen from the histogram of Fig. 2 that the histogram after grayscale is smaller than the original histogram y coordinate value, and the histogram has some slight difference.

The Lena grayscale image shown in Fig. 2 is encrypted and decrypted. Figure 3 shows the encryption and decryption ciphertext, the upper left side of Fig. 3 is the original image grayscale image and the upper right is the decrypted image. There is no difference between the two on the original image. From the histogram, there is no difference between the two, indicating that this method can restore the image very well after decryption. The middle of Fig. 3 is an encrypted image of the grayscale image. From the perspective of the encryption and the original image, there is no connection between the two. From the histogram, there is no relationship between the two. Compared to Fig. 3, it can be seen that the encryption algorithm encrypts the plaintext image very well and does not have any meaningful content visually. It can be seen from the encryption and decryption maps in the two figures that the two decrypted images can be recovered without distortion. In addition, from the histogram of the two images, the histogram before encryption shows uneven distribution and obvious peaks and troughs, indicating that the correlation between adjacent pixels is strong. The histogram obtained by the encryption has a stable distribution, similar to noise, indicating that the correlation between adjacent pixels is weak, so that the attacker cannot obtain the useful information at all, thereby preliminarily illustrating the effectiveness of the encryption algorithm.

In order to better measure the encryption and decryption effect of this method, this paper uses Color Photo to verify the effectiveness of the encryption and decryption methods. Figure 4 shows the encryption and decryption effects of Color Photo. It can be seen from the results in Fig. 4 that the difference between the histogram and the grayscale image of the color life photograph is larger than that of Fig. 3. However, starting from the grayscale image, the performance of the grayscale-encrypted and decrypted graph is not the same as that of Fig. 3, and it is relatively smooth on the histogram of the encrypted plaintext image. It can be seen from the encryption and decryption process of life graph that this paper has achieved good results.

Information entropy refers to the measure and method of randomness in information theory. If the randomness

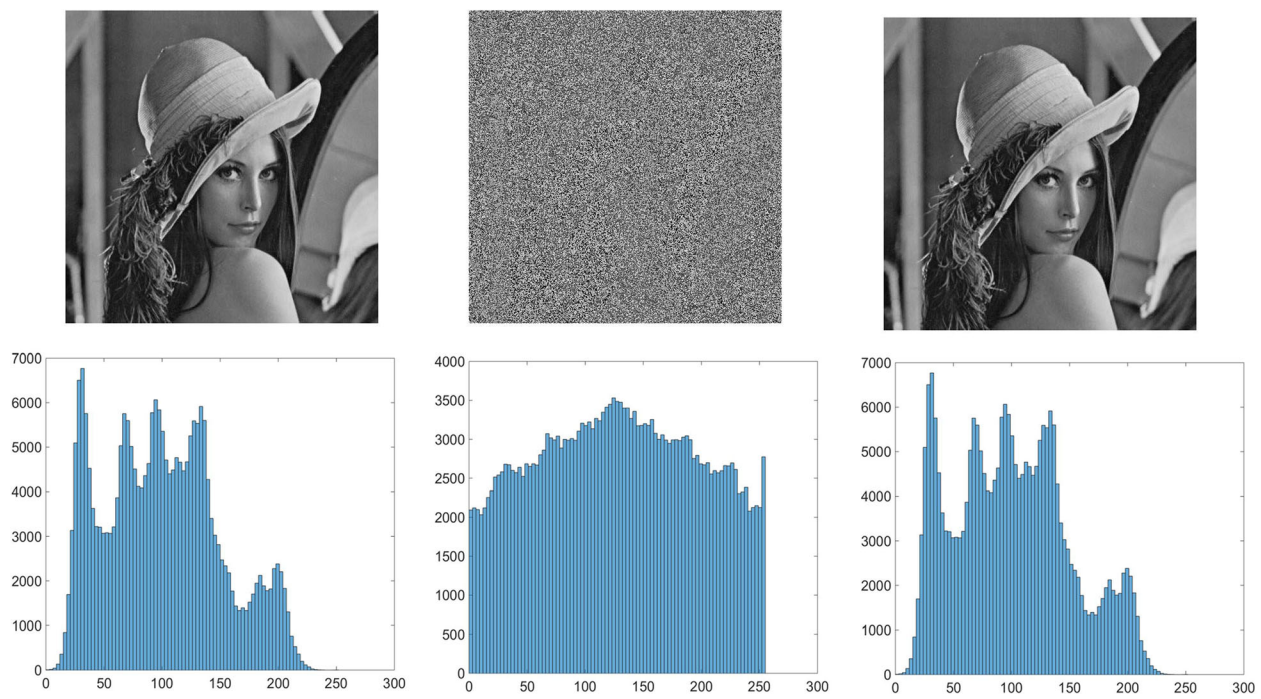

Fig. 3 Comparison before and after encryption and decryption

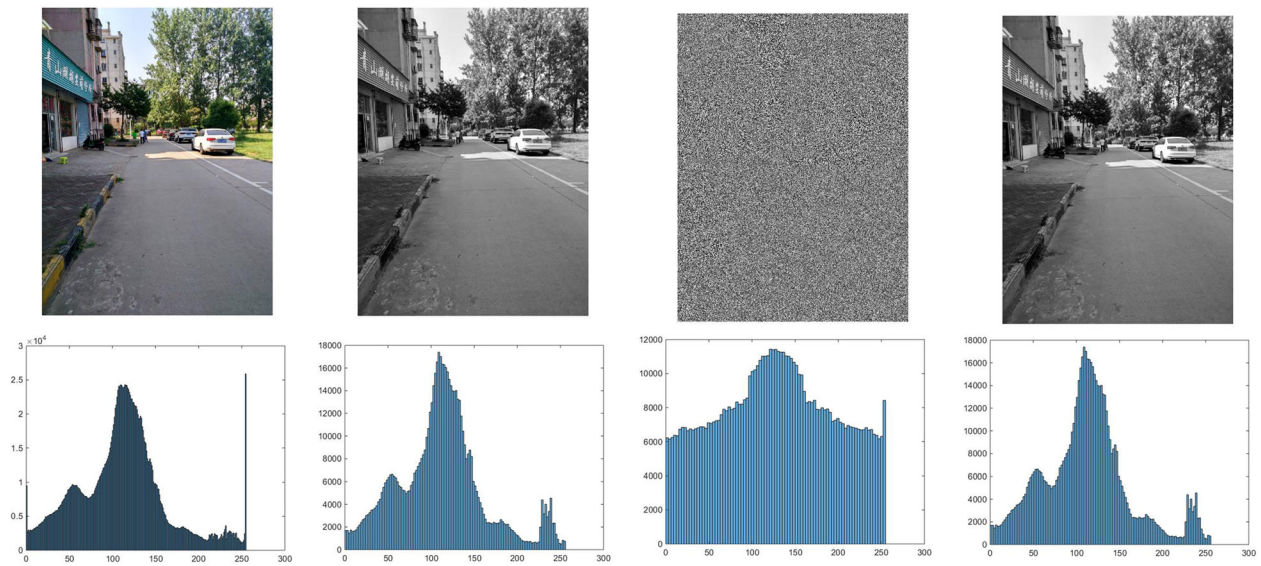

Fig. 4 Comparison of encryption and decryption of Color Photo

of a set of data is higher and the data is more chaotic, then the information entropy is larger. If the information is more regular, the information entropy will be smaller. The value of information entropy is in the interval [0 1]. If the information entropy of a system is 1, it means that the system has no regularity at all. If the information entropy is 0, it means that the system does not have any randomness or irregularity. The result of confidentiality of plaintext and ciphertext can be described by the value of information entropy. The greater the information entropy, the better the confidentiality. The calculation method of information entropy is as follows:

$$H(s) = \sum_{i=0}^{2^{N-1}} p(s_i)\ \log_2 p(s_i)$$

Since there are 2^8 possible values for each pixel, the entropy is 8 when there is no pixel correlation at all. But in general, the actual information entropy is less than 8 because the digital image cannot be completely random. For images representing real objects or characters, the information entropy is generally between 2 and 4. The information entropy of the abovementioned Lena image and life photo is calculated. Table 1 shows the entropy values of the original grayscale image, ciphertext, and decrypted image. From the results of Table 1, it can be seen that the entropy of the gray and decryption figures before encryption is about 2.3, indicating that there is a strong correlation between the various elements of the graph. But the information entropy of the ciphertext is very close to the extreme value of 8, indicating that the encrypted images are close to random distribution, and the security is higher.

Table 1 Entropy value comparison table before and after transformation

	Original grayscale	Ciphertext	Decrypt
Lena	2.34	7.95	2.37
Life	2.11	7.98	2.21

The experimental simulation of the method uses parameters $\mu = 3.87$, $a = 0.564$, and $b = 0.37$ in the process of encryption and decryption, wherein the value range of the parameter u_1 is defined between (3,4], and the value of a and b is between (0 1). Theoretically, the key space of this method is infinite. However, considering the limitation of computing performance and precision in practical application, the accuracy will be limited when the actual value is taken. The key of this method uses the key of (u_1, a,b) in the process of confusion and scrambling, so the key space can reach the range of 10^{45}, and its key space is sufficient to resist the general exhaustive attack.

The sensitivity of key is an important index of encryption. The key sensitivity analysis mainly refers to the security analysis in the process of encryption and decryption using the wrong key. Because of the sensitivity of the initial value of the chaotic map, the method of this paper has a good key sensitivity from the theoretical level. In the decryption process, the decryptor must correctly provide the initial value a of L1 and L2 during the two iterations, and the other parameters remain unchanged. Figure 5 shows the ciphertext before and after the change of a is 0.564 and 0.565. The left side is the original parameter and the right is the parameter after the transformation of a value. Although we can see the difference from the picture, it is not obvious. The correlation between the two ciphertext before and

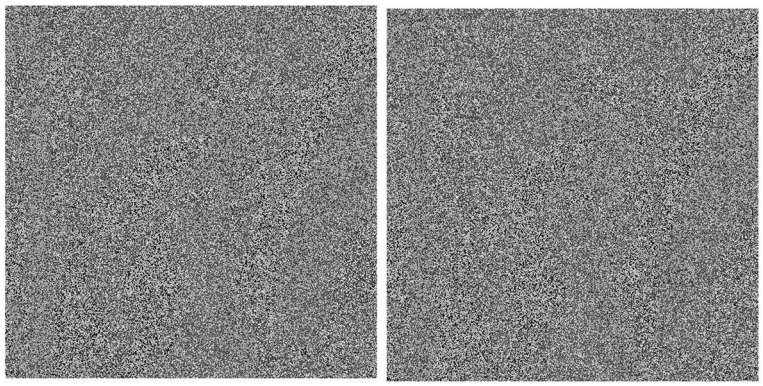

Fig. 5 The contrast of Lena's ciphertext before and after the change

after calculation can be obtained, the correlation coefficient is − 0.0013, indicating that there is almost no correlation between the two. This indicates that the key is sensitive to the coefficients and the security of the encryption method in this paper.

4 Conclusions

With the rapid development of communication and computer network technology, the problem of secure transmission of information has received more and more attention, and encryption is an effective means to ensure the secure transmission of information. Due to the large amount of data, strong correlation and high redundancy of the image itself, the traditional encryption method is not suitable for image encryption, so it is necessary to seek a new solution. The birth and development of chaos theory has brought hope to the research of image encryption. The high sensitivity to initial conditions, the history of each state, and the pseudorandomness are typical features of chaos, which coincide with the basic requirements of cryptography, namely, confusion and diffusion. Therefore, since the introduction of chaos theory into image encryption in the 1990s, chaotic image encryption technology has flourished. In this context, a digital image method based on double logistic chaotic mapping is proposed. Through the size of the key space, the sensitivity of the method to the key, the pixel correlation of the encrypted image and the entropy, the security, and reliability analysis of the connection bar shows that the method has a definite advantage on the reliability and security of the Lena image and the life illumination image.

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Funding

The paper is supported in part by Gaoyuan Discipline of Shanghai–Environmental Science and Engineering (Resource Recycling Science and Engineering), Discipline of Management Science and Engineering of Shanghai Polytechnic University (Grant No. XXKPY1606).

Availability of data and materials

Please contact author for data requests.

Authors' contributions

All authors take part in the discussion of the work described in this paper. The author HP wrote and revised the paper in a different version. The author CJ did part of the experiments of the paper respectively. All authors read and approved the final manuscript.

Authors' information

Hailan Pan was born in Putian, Fujian, P.R. China, in 1979. She received her bachelor's degree from Fudan University, P.R. China. Now, she studies in School of Computer Engineering and Science, Shanghai University and works in School of Economics and Management, Shanghai Polytechnic University. Her research interests include e-commerce, big data analysis, workflow, and parallel computing.
E-mail: panhailan@sspu.edu.cn.
Yongmei Lei, Professor, Doctoral tutor, received the Ph.D from Xi'an Jiaotong University, P.R. China. Now, she works in School of Computer Engineering and Science, Shanghai University. Her research interests include high-performance computing, grid computing, and network security.
E-mail:lei@shu.edu.cn.
Jian Chen was born in Lishui, Zhejiang, P.R. China, in 1977. He received the Ph.D. from Derby University, U.K. Now, he works in School of Economics and Management, Shanghai Polytechnic University. His research interests include business intelligence, e-commerce, and big data analysis.
E-mail: chenjian@sspu.edu.cn.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]School of Computer Engineering and Science, Shanghai University, No. 99, Shangda Rd, Baoshan District, Shanghai, China. [2]Research Center of Resource Recycling Science and Engineering, Shanghai Polytechnic University, No. 2360, Jinhai Rd, Pudong New District, Shanghai, China. [3]School of Economics and Management, Shanghai Polytechnic University, No. 2360, Jinhai Rd, Pudong New District, Shanghai, China.

Received: 8 September 2018 Accepted: 28 November 2018
Published online: 13 December 2018

References

1. R.M. Redlich, M.A. Nemzow, *Digital information infrastructure and method for security designated data and with granular data stores: US, US9734169 [P]* (2017)
2. Z. Han, S. Huang, H. Li, et al., Risk assessment of digital library information security: A case study [J]. Electron. Libr. **34**(3), 471–487 (2016)

3. Zhou C, Guo Y, Huang W, et al. Information security defense method of electric power control system based on digital watermark[C]// International Conference on Materials Engineering, Manufacturing Technology and Control. 2016
4. E. Chisanga, E.K. Ngassam, Towards a conceptual framework for information security digital divide[C]// Ist-Africa week conference. IEEE, 1–8 (2017)
5. T. Caulfield, C. Ioannidis, D. Pym, Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper). In International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg (2016), pp. 271-279
6. Z. Cai, D. Huang, Research on DES Data Encryption Technology in Network Information Security [J]. Computer Measurement & Control. **25**, 241-247 (2017)
7. Sun Y Q, Wang X H. Information encryption technology with strong robustness based on QR code and matrix mapping [J]. Packaging Engineering. **38**, 194-199 (2017)
8. S.W. Lee, S.M. Park, K.B. Sim, et al., Smart Door Lock Systems using encryption technology [J]. **27**(1), 65–71 (2017)
9. Z. Wen, L.I. Taoshen, Z. Zhang, An image encryption technology based on chaotic sequences [J]. Comput Eng. **31**(10), 130–132 (2005)
10. Y.Y. Wang, Y.R. Wang, Y. Wang, et al., Optical image encryption based on binary Fourier transform computer-generated hologram and pixel scrambling technology [J]. Optics & Lasers in Engineering **45**(7), 761–765 (2007)
11. X.Y. Zhang, W. Chao, L.I. Su-Mei, et al., Image encryption technology on two-dimensional cellular automata [J]. Journal of Optoelectronics Laser **19**(2), 242–245 (2008)
12. J. Ahmad, M.A. Khan, S.O. Hwang, J.S. Khan, A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. Neural Computing and Applications **28**(S-1), 953–967 (2017)
13. X. Sixing, S. Xin, L. Bing, et al., New image encryption technology of image based on computer generated hologram [J]. Laser & Optoelectronics Progress **49**(4), 040902 (2012)
14. J.M. Matthews, A.F.J. Moffat, WR 40: Coherence or chaos? [J]. Astronomy & Astrophysics **283**, 493–507 (1994)
15. T. Habutsu, Y. Nishio, I. Sasase, et al., *A secret key cryptosystem by iterating a chaotic map[C]// the workshop on advances in cryptology-Eurocrypt*. Springer-Verlag, **13**(1),1-5 (1991)
16. J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps [J]. International Journal of Bifurcation & Chaos **08**(06), 9800098 (1998)
17. Ismail I A, Amin M, Diab H. A digital image encryption algorithm based a composition of two chaotic logistic maps [J]. International Journal of Network Security, 2010, 11(1):1–10
18. S. Fuyan, L. Zongwang, Digital image encryption with chaotic map lattices [J]. Chinese Physics B **20**(4), 132–138 (2011)
19. A.V. Diaconu, K. Loukhaoukha, An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher [J]. Mathematical Problems in Engineering **2013**(6), 1–10 (2013)
20. X. Wang, L. Lintao, Cryptanalysis and improvement of a digital image encryption method with chaotic map lattices [J]. Chinese Physics B **22**(5), 198–202 (2013)
21. T.K. Sun, X.G. Shao, X.Y. Wang, A novel binary image digital watermarking algorithm based on DWT and chaotic encryption[C]// the, international conference for young computer scientists. IEEE Computer Society, 2797–2802 (2008)
22. L.I. Yu-Zhen, X. Jin, G. Zhao, et al., Color image encryption scheme based on zigzag transformation and chaotic map [J]. Computer Engineering & Design. **37**, 2001-2006 (2016)
23. L. Liu, S. Xiao, L. Zhang, et al., Digital chaos-masked optical encryption scheme enhanced by two-dimensional key space [J]. Opt. Commun. **398**, 62–66 (2017)
24. M. Zhao, X. Tong, A multiple chaotic encryption scheme for image[C]// international conference on wireless communications NETWORKING and Mobile computing. IEEE, 1–4 (2010)
25. G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos, Solitons Fractals **21**(3), 749–761 (2004)
26. K.F. Wang, S. Zhuang, X.R. Zhao, JPEG image encryption algorithm based on three-dimensional multi-chaotic system [J]. Applied Mechanics & Materials **734**, 554–557 (2015)
27. C. Xiuli, G. Zhihua, Y. Ke, et al., An image encryption scheme based on three-dimensional Brownian motion and chaotic system [J]. Chinese Physics B **26**(2), 99–113 (2017)